⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平4−149690

⑤Int.Cl.⁵		識別記号	庁内整理番号	㊸公開 平成4年(1992)5月22日
G 06 K	17/00	S	6711−5L	
G 07 F	7/08			
	7/12			
G 07 G	1/12	321 P	8921−3E	
			8111−3E	G 07 F 7/08 C
			8111−3E	M

審査請求 未請求 請求項の数 1 (全7頁)

㊹発明の名称　記録データ処理装置

㉑特　願　平2−271462
㉒出　願　平2(1990)10月9日

㉜発明者　大石　和弘　東京都西多摩郡羽村町栄町3丁目2番1号　カシオ計算機株式会社羽村技術センター内
㉛出願人　カシオ計算機株式会社　東京都新宿区西新宿2丁目6番1号

明　細　書

1．発明の名称

記録データ処理装置

2．特許請求の範囲

入力される暗号データを設定自在に記憶する暗号データ記憶手段と、この暗号データ記憶手段に記憶された暗号データに基づき、記録媒体のデータを暗号化あるいは復号化して記録媒体に対して読み書きする読み書き手段と、各種命令に従って各種処理を実行する実行制御手段と、各種命令が正常命令か否かを判別する判別手段と、この判別手段で各種命令が正常命令でないと判別された際に上記暗号データ記憶手段に記憶された暗号データを消去する消去手段とを具備したことを特徴とする記録データ処理装置。

3．発明の詳細な説明

［産業上の利用分野］

この発明は、例えばプリペイドカードリーダ・ライタ等の記録データ処理装置に関する。

［従来の技術］

ＥＣＲやＰＯＳターミナル等に接続されるプリペイドカードリーダ・ライタは、暗号化・復号化ルーチンプログラムをＲＯＭに記憶し、プリペイドカードに対して読み込み、暗号データの復号、金額減算、暗号化、書き込み、という処理を行なうものであった。

［発明が解決しようとする課題］

そのため、プリペイドカードリーダ・ライタを盗んでＲＯＭプログラムを解析して、プリペイドカードに金額データを書き込む命令コードを探り当て、不正にプリペイドカードを発券するという犯罪が発生している。

この発明の課題は、プリペイドカードリーダ・ライタが盗難にあっても、プリペイドカードが不正に発券されることを防止できるようにすることである。

［課題を解決するための手段］

この発明の手段は次の通りである。

暗号データ記憶手段1（第1図の機能ブロック図を参照、以下同じ）は、例えばＲＡＭにより構

成され、入力される暗号データを設定自在に記憶する。

読み書き手段２は、例えば磁気カードリーダ・ライタ等であり、暗号データ記憶手段１に記憶された暗号データに基づき、磁気カード等の記録媒体のデータを暗号化あるいは復号化し、記録媒体に対して読み書きする。

実行制御手段３は、各種命令に従って各種処理を実行する。

判別手段４は、各種命令が例えばＲＯＭに記憶された正常命令か否かを判別する。

消去手段５は、判別手段４で各種命令が正常命令でないと判別された際に上記暗号データ記憶手段１に記憶された暗号データを消去する。

［作用］

この発明の手段の作用は次の通りである。

暗号データ記憶手段１に記憶された暗号データに基づいて読み書き手段２が記録媒体のデータを暗号化・復号化し、磁気カード等の記録媒体に対して読み書きし、実行制御手段３が各種命令に従って各種処理を実行する。

判別手段４で各種命令が正常命令でないと判別された際に、消去手段５は上記暗号データ記憶手段１に記憶された暗号データを消去する。

従って、プリペイドカードリーダ・ライタが盗難にあい、プリペイドカードに対して不正にデータを書き込もうとしても、異なった命令が指示された際に暗号データが消去されるので、プリペイドカードに正規のデータを書き込めず、プリペイドカードが不正に発券されることを防止できる。

［実施例］

以下、実施例を第２図乃至第５図に示す図面に基づいて説明する。なお、この実施例はプリペイドカードリーダ・ライタにより構成された記録データ処理装置を示している。

第２図は、プリペイドカード端末装置の回路構成を示すブロック図である。このプリペイドカード端末装置は例えばＥＣＲである。

同図において、鉛入力装置１０は図示しないが「０」～「９」等の数値データを入力するテンキー、各種処理を指定するファンクションキー、売上データの部門別登録を指定する部門キー、各モードを指定するモードキー、およびその他のキーを備えている。しかして、鉛入力装置１０はキー入力を行なうと、これに応じたキー入力信号をＣＰＵ１１に出力する。

ＣＰＵ１１は、鉛入力装置１０から出力されるキー入力信号に応じて登録処理、定額引落し処理等の各種処理を実行する。これらの各種処理はＲＯＭ１２に予め記憶した制御プログラムに基づいて実行される。

ＲＡＭ１３は各種データを記憶するもので、ＣＰＵ１１により読出し／書込みが制御される。プログラムカードＩ／Ｆ（インターフェイス）１４は、プログラムカード１５とＣＰＵ１１とのデータ授受を行なう。プログラムカード１５は、暗号データを記憶したＲＯＭカードまたはＲＡＭカードにより構成されている。リーダ・ライタＩ／Ｆ１６はプリペイドカードリーダ・ライタ１７とＣＰＵ１１とのデータ授受を行なう。表示部１８は例えば蛍光表示パネルにより構成されるもので、ＣＰＵ１１から出力される表示データを表示する。プリンタ１９はＣＰＵ１１から出力される印字データを印字する。

第３図は、プリペイドカードリーダ・ライタ１７の回路構成を示すブロック図である。このプリペイドカードリーダ・ライタ１７は、例えば磁気カードにより構成されるプリペイドカードに対して金額データの読み込み及び書き込みを行なうものである。同図において、ＣＰＵ２０は図示しない内部ＲＯＭに記憶した制御プログラムに基づいて各部を制御するもので、リーダ・ライタメカニズム２１、ＲＯＭ２２、ＲＡＭ２３、およびＩ／Ｆ２４が接続されている。

リーダ・ライタメカニズム２１は、プリペイドカードに記録されたデータを読み込み又は書き込むための磁気ヘッド、カード搬送機構等を内蔵するものである。この場合、プリペイドカードにはカード種類，発行番号，金額データ等のデータが記録されている。

ＲＯＭ２２には、例えば第３図に示すように暗号ダウンロードコマンド、読み込みコマンド、書き込みコマンド、エジェクトコマンド、および暗号ルーチン等の各種制御情報が予め記憶されている。この実施例において、暗号ダウンロードコマンドはプリペイドカード端末装置から送信された暗号データをＲＡＭ２３のエリアにセーブすることを指示するコマンドである。読み込みコマンドは、プリペイドカードのデータら読み込んで暗号化して送信することを指示するコマンドである。書き込みコマンドは、プリペイドカードに金額データを書き込むことを指示するコマンドである。エジェクトコマンドは、プリペイドカードを装置の外に排出することを指示するコマンドである。暗号ルーチンは、ＲＡＭ２３に記憶された暗号データに基づいてプリペイドカードに書き込むデータを暗号化し、或いはプリペイドカードから読み込んだ暗号化されたデータを元のデータに復号化するためのプログラムである。

ＲＡＭ２３は、プリペイドカード端末装置から初期設定時にセーブされた暗号データを記憶するもので電池２３ａから記憶保持のための電源が供給されている。

Ｉ／Ｆ２４はプリペイドカード端末装置と接続されてデータ通信を行なうものである。

次に、第４図および第５図に示すフローチャートに基づき上記実施例の動作を説明する。

第４図を参照してプリペイドカード端末装置の動作を説明する。まず、ステップＡ１ではＩＮＩＴ　ＳＷ（イニシャライズ・スイッチ）が操作されたか否かが判断される。ＩＮＩＴ　ＳＷは、プログラムカード１５に記憶された暗号データをプリペイドカードリーダ・ライタ１７に転送してＲＡＭ２３にセーブして初期化する際に操作するスイッチである。このステップＡ１でＹＥＳと判断された場合はステップＡ２に進み、ＮＯの場合はステップＡ６に進む。

ここで、プリペイドカードリーダ・ライタ１７を初期化するためにＩＮＩＴ　ＳＷを操作したとする。これにより、ステップＡ２に進み、プログラムカード１５がＩ／Ｆ１４と接続されているか否かが判断される。プログラムカードが有る場合は、ステップＡ２でＹＥＳと判断されてステップＡ３に進む。もし、プログラムカードがない場合はＮＯとなり、ステップＡ８によりエラー表示が実行されてステップＡ１に戻る。

ステップＡ３においては、プログラムカード１５に記憶された暗号データがＩ／Ｆ１４を介してＣＰＵ１１に読み出される。続くステップＡ４では、プログラムカード１５から読み出された暗号データと暗号ダウンロードコマンドとをＩ／Ｆ１６を介してプリペイドカードリーダ・ライタ１７に転送する。

次に、ステップＡ５ではデータが正常に転送されたか否かが判断され、正常であればステップＡ６に進み、正常でなければステップＡ９のエラー表示に進む。

ステップＡ６においては、プリペイドカードリーダ・ライタ１７に対して読み込みコマンドを送信し、読み込みコマンドに応じてプリペイドカードリーダ・ライタ１７から送信される結果データを受信する。この場合、金額データが入力されていないので読み込みコマンドは送信されない。

ステップＡ７では読み込みが未完か否かが判断される。このステップＡ７で、読み込みが未完でＹＥＳと判断された場合はステップＡ１に戻り、ＮＯの場合はステップＡ１０に進む。この場合、読み込みコマンドを送信していないのでＹＥＳと判断されてステップＡ１に戻る。

次に、プリペイドカードから金額データを引落とす場合は、ＩＮＩＴ　ＳＷをＯＦＦしておき、個入力装置１０により金額データを入力する。これにより、ステップＡ１でＮＯと判断されてステップＡ６に進む。

ステップＡ６においては、プリペイドカードリーダ・ライタ１７に対して読み込みコマンドを送信して残高データの読み込みを指示し、送信されてくる残高データを受信する。

ステップＡ７ではプリペイドカードリーダ・ライタ１７からの読み込みが未完か否かが判断され

る。このステップＡ７で、ＹＥＳと判断された場合はステップＡ１に戻り、ＮＯの場合はステップＡ１０に進む。

ステップＡ１０では、プリペイドカードリーダ・ライタ１７から送信されたデータが正常な復号化データか否かが判断される。即ち、残高データを暗号データに基づいて解析し、正常な復号化データか否かを判断する。このステップＡ１０でＹＥＳと判断されるとステップＡ１１に進み、ＮＯの場合はステップＡ１５のエラー表示に進む。

ステップＡ１１においては、残高データから売上データを減算することが可能か否かが判断される。ステップＡ１１でＹＥＳと判断されるとステップＡ１２に進み、残高データが売上データよりも小さくＮＯと判断されるとステップＡ１５のエラー表示に進む。

ステップＡ１２では、プリペイドカードの残高データから売上データを減算し、減算後の残高データと書き込みコマンドとを送信して残高データの書き込みを指示し、プリペイドカードリーダ・ライタ１７から送信されてくる結果ＯＫデータを受信する。

ステップＡ１３では正常書込み完了か否か、即ちプリペイドカードリーダ・ライタ１７が結果ＯＫデータを送信したか否かが判断される。このステップＡ１３でＹＥＳと判断された場合はステップＡ１４に進み、ＮＯの場合はステップＡ１５に進む。

ステップＡ１４において、プリペイドカードリーダ・ライタ１７に対してカードエジェクトコマンドを送信し、ステップＡ１に戻る。

次に、第５図を参照してプリペイドカードリーダ・ライタ１７の動作を説明する。

ステップＢ１では、プリペイドカード端末装置からのコマンドを受信したか否かが判断される。コマンドを受信していない場合はステップＢ１が繰り返し実行される。そして、何かのコマンドが受信されると、ステップＢ２に進む。

ステップＢ２においては、受信されたコマンドがＲＯＭ２２に記憶した「暗号ダウンロードコマンド」と一致するか否かが判断される。このステップＢ２で、ＹＥＳと判断されるとステップＢ３に進む。

ステップＢ３では、暗号ダウンロードコマンドの後に送信されてくる暗号データをＲＡＭ２３にセーブし、ステップＢ１４に進む。

ステップＢ１４において、結果ＯＫを示すデータをＣＰＵ２０に内蔵された送信バッファ（図示せず）にセットし、次のステップＢ１７により送信バッファの内容をプリペイドカード端末装置に送信する。ステップＢ１７の終了後はステップＢ１に戻る。

また、ステップＢ２でＮＯと判断された場合はステップＢ４に進む。ステップＢ４では、受信されたコマンドがＲＯＭ２２に記憶した「読み込みコマンド」と一致するか否かが判断される。このステップＢ４で、ＹＥＳと判断されるとステップＢ５に進む。

ステップＢ５では、ＲＡＭ２３の暗号データエリアが正常か否かが判断される。ステップＢ５で暗号データエリアが正常である場合はステップＢ６に進み、暗号データエリアがクリアされて正常でなければステップＢ１６に進む。

ステップＢ６においては、暗号ルーチンをＲＯＭ２２から読み出し、ＲＡＭ２３に記憶された暗号データに基づいてプリペイドカードから読み出した残高データを復号化する。

ステップＢ７では、復号化された残高データをＣＰＵ２０の送信バッファにセットし、次のステップＢ１７により送信バッファの内容をプリペイドカード端末装置に送信する。ステップＢ１７の実行後はステップＢ１に戻る。

次のステップＢ８により、受信されたコマンドがＲＯＭ２２に記憶した「書き込みコマンド」と一致するか否かが判断される。このステップＢ８で、ＹＥＳと判断されるとステップＢ９に進む。

ステップＢ９においては、ステップＢ５と同様に、ＲＡＭ２３の暗号データエリアが正常か否かが判断される。ステップＢ９で暗号データエリアが正常であればステップＢ１０に進み、正常でな

ければステップＢ１６に進む。

ステップＢ１０において、暗号ルーチンをＲＯＭ２２から読み出し、ＲＡＭ２３に記憶された暗号データに基づいてプリペイドカード端末装置から送信された残高データを暗号化する。

ステップＢ１１では、暗号化された残高データをリーダ・ライタメカニズム２１によりプリペイドカードに書き込み、ステップＢ１４に進む。

ステップＢ１４においては、結果ＯＫを示すデータをＣＰＵ２０に内蔵された送信バッファにセットする。次のステップＢ１７では送信バッファの内容をプリペイドカード端末装置に送信し、ステップＢ１に戻る。

また、上記ステップＢ８でＮＯと判断された場合はステップＢ１２に進む。ステップＢ１２においては、受信されたコマンドがＲＯＭ２２に記憶した「エジェクトコマンド」と一致するか否かが判断される。このステップＢ１２で、ＹＥＳと判断されるとステップＢ１３に進み、リーダ・ライタメカニズム２１が作動してプリペイドカードが外部に排出される。ステップＢ１３の実行後は、上述と同様に、ステップＢ１４，Ｂ１７が実行される。

しかして、ステップＢ１２でＮＯと判断される場合は、プリペイドカード端末装置から正常でないコマンドが送信されたことになるので、ステップＢ１５に進み、ＲＡＭ２３の暗号データエリアをクリアしてプリペイドカードリーダ・ライタ１７を使用不可とする。

次のステップＢ１６では、暗号データが正常でないことを示す暗号ＮＧ情報をＣＰＵ２０の送信バッファにセットする。ステップＢ１７においては、上述と同様に送信バッファの内容をプリペイドカード端末装置に送信し、ステップＢ１に戻る。

従って、ステップＢ１５によりＲＡＭ２３に記憶された暗号データがクリアされた後は、ステップＢ５，Ｂ９が実行された時に夫々ＮＯと判断されるので、プリペイドカードに記録されたデータの復号化も暗号化もできず、プリペイドカードが不正に発券されることを防止できる。

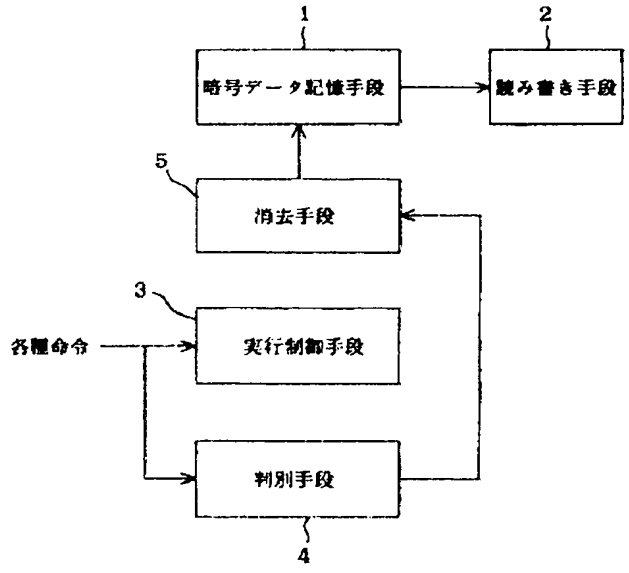
［発明の効果］

以上詳述したように、この発明によればプリペイドカードリーダ・ライタが盗難にあい、プリペイドカードに対して不正にデータを書き込もうとしても、異なった命令が指示された際に暗号データが消去されるので、プリペイドカードに正規のデータを書き込めず、プリペイドカードが不正に発券されることを防止できる。

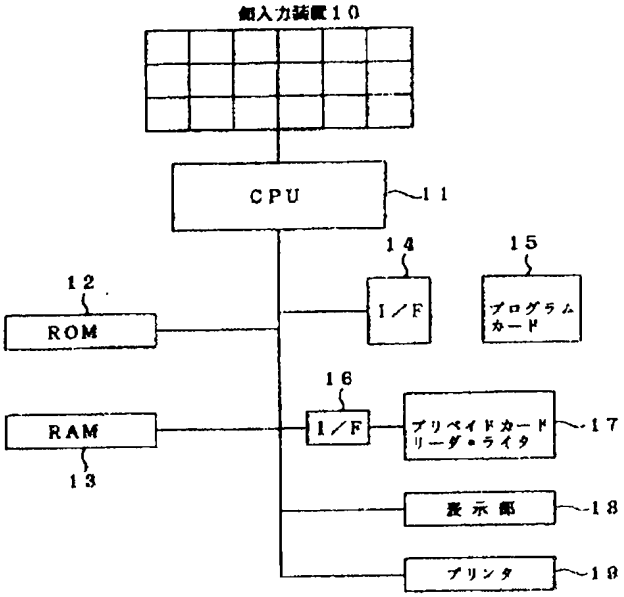
４．図面の簡単な説明

図面は実施例を示すもので、第１図は本発明の機能ブロック図、第２図はプリペイドカード端末装置の回路構成を示すブロック図、第３図はプリペイドカードリーダ・ライタの回路構成を示すブロック図、第４図および第５図は動作を示すフローチャートである。

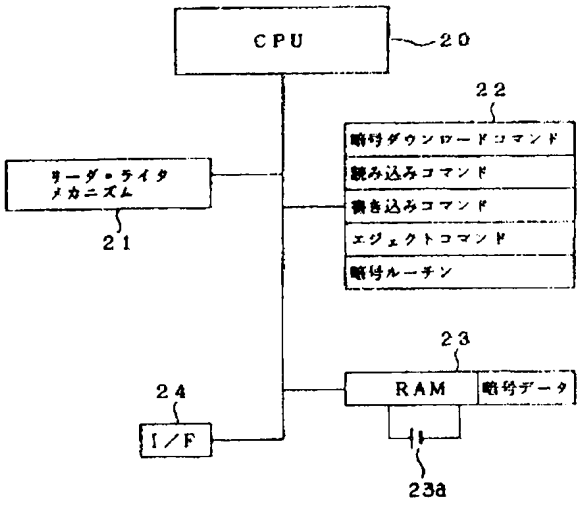
１…暗号データ記憶手段、２…読み書き手段、３…実行制御手段、４…判別手段、５…消去手段、２０…ＣＰＵ、２１…リーダ・ライタメカニズム、２２…ＲＯＭ、２３…ＲＡＭ。



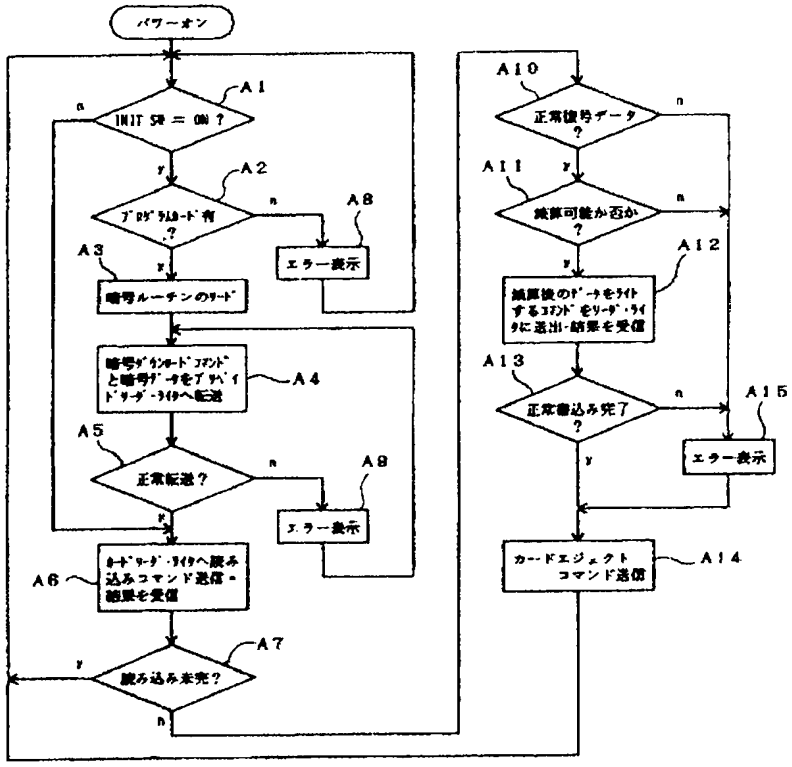
第１図


鍵入力装置10
CPU
11
12
ROM
13
RAM
14
I/F
15
プログラムカード
16
I/F
プリペイドカードリーダ・ライタ
17
表示部
18
プリンタ
19

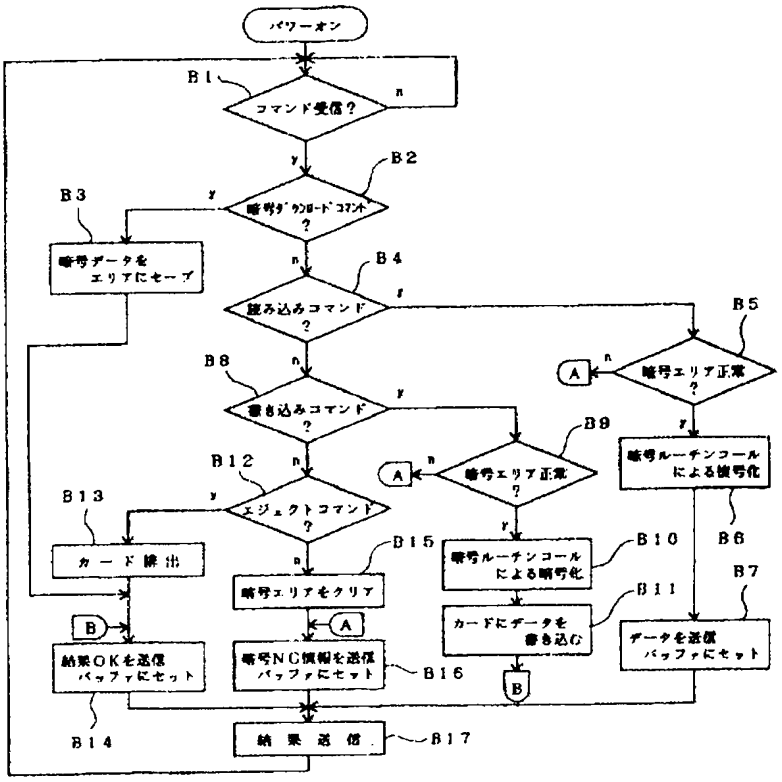
第2図


CPU
20
22
暗号ダウンロードコマンド
読み込みコマンド
書き込みコマンド
エジェクトコマンド
暗号ルーチン
リーダ・ライタメカニズム
21
23
RAM
暗号データ
24
I/F
23a

第3図


パワーオン
A1
INIT SW = ON ?
A2
プログラムロード有?
A8
エラー表示
A3
暗号ルーチンのリード
暗号ダウンロードコマンドと暗号データをプリペイドリーダ・ライタへ転送
A4
A5
正常転送?
A9
エラー表示
カードリーダ・ライタへ読み込みコマンド送信・結果を受信
A6
A7
読み込み未完?
A10
正常復号データ?
A11
演算可能か否か?
A12
演算後のデータをライトするコマンドをリーダ・ライタに送出・結果を受信
A13
正常書込み完了?
A15
エラー表示
カードエジェクトコマンド送信
A14

第4図


パワーオン
B1
コマンド受信？
n
y
B2
暗号ダウンロードコマンド？
y
B3
暗号データをエリアにセーブ
n
B4
読み込みコマンド？
y
B5
暗号エリア正常？
A
n
y
B6
暗号ルーチンコールによる復号化
B7
データを送信バッファにセット
n
B8
書き込みコマンド？
y
B9
暗号エリア正常？
A
n
y
B10
暗号ルーチンコールによる暗号化
B11
カードにデータを書き込む
B
n
B12
エジェクトコマンド？
y
B13
カード排出
B14
結果OKを送信バッファにセット
B
n
B15
暗号エリアをクリア
A
B16
暗号NG情報を送信バッファにセット
B17
結果送信

第5図